In re Patent Application of
LIARDET ET AL.
Serial No. **09/506,158**
Filed: **FEBRUARY 17, 2000**
______________________________/

REMARKS

The Examiner is thanked for the thorough examination of the present application. In view of the arguments presented in detail below, it is submitted that all of the claims are patentable.

I. The Claimed Invention

The present invention is directed to and electronic circuit for a cryptography coprocessor. As recited in independent Claim 17, for example, the electronic circuit includes a plurality of input/output registers having a scrambling register for receiving digital key data. More particularly, the digital key data includes a digital key and a plurality of scrambling bits intermixed with the digital key. The electronic circuit further includes an input register for receiving message data to be processed by the encryption or decryption operation, and a key register for receiving the digital key data for use in the encryption or decryption operation. A multiplexer transfers data between the plurality of input/output registers and the input register and the key register. Moreover, a processor is connected to the scrambling register, the input register, and the key register and performs the encryption or decryption operation on the message data in the input register based upon the digital key data and the scrambling bits. The electronic circuit further includes a controller for controlling the plurality of input/output registers, the multiplexer and the processor, and an output register to transmit the result of the encryption or decryption operation to the plurality of input/output registers through the multiplexer.

The intermixed scrambling bits advantageously secure the loading of the digital key into the input/output registers. Yet, by separately storing the scrambling bits in the scrambling register, the processor may readily determine the digital key from the contents of the key register and the scrambling register, as discussed on pages 12 and 13 of the originally filed specification, for example. Independent Claim 11 is directed to a related electronic circuit, and independent Claims 25 and 30 are directed to related methods. Similar to Claim 17, each of these claims recites that the scrambling bits are intermixed with the digital key.

II. The Claims Are Patentable

The Examiner rejected independent Claims 11, 17, 25, and 30 based upon the prior art illustrated in FIG. 3 of the application and U.S. Patent No. 6,144,744 to Smith, Sr. et al. (hereafter "Smith"). While the Examiner acknowledges that the prior art shown in FIG. 3 of the present application fails to teach or fairly suggest intermixing scrambling bits with a digital key, the Examiner contends that Smith provides this noted deficiency.

Smith discloses a method and apparatus for securely transferring objects (i.e., master keys) between different cryptographic processing modules. The master key transfer is accomplished using the Dieffie-Hellman key exchange protocol which allows a module to create a transport key for encrypting items to be transferred to a receiving module. Thus, the method of Smith allows the two modules to build a transport key to securely transfer a master key encrypted with the transport key.

In the first Office Action mailed January 15, 2004, the Examiner noted a transport key register **1620** in FIG. 16 of Smith, and he contended that this register is a scrambling register for storing scrambling bits as recited in the above-noted independent claims. In response, Applicants noted in the Amendment filed April 15, 2004 that Smith teaches at col. 15, lines 40-45 and col. 17, lines 50 through col. 18, line 30 that the transport key stored in the register **1620** is merely a secret key used to encrypt an object protection key to be transferred between the modules. The transport key is not transferred with the encrypted object protection key between the modules. As such, the transport key is neither included as part of any digital key data to be transmitted, nor is it intermixed with the object protection key, as recited in each of the above independent claims. It was therefore noted that the selective combination of references proposed by the Examiner failed to teach or fairly suggest all of the elements recited in the above-noted independent claims.

The Examiner now contends in the final Office Action that a BTK register **1614** discussed at col. 16, lines 13-36 of Smith is equivalent to the scrambling register, and that this BTK register receives digital key data comprising a digital key and scrambling bits intermixed therewith, as recited in the above-noted independent claims. However, the Examiner provides no explanation for this contention beyond pointing to the above-noted text of Smith. This text is reproduced below for convenience:

> "FIG. 17 shows the general procedure **1700** for transferring a key part (such as MK1 or AMK1) from one crypto module **102** to another.
>
> First, using the procedure to be described below, an authority establishes a basic transport key (BTK) as a shared secret between the source and target modules **102** (step **1702**). At the end of this step, the transport key BTK is stored in the BTK register **1614** of each crypto module **102** involved in the transfer, but is not itself accessible to the authority **104**.
>
> The authority **104** then extracts the key part from the appropriate master key register of the source module **102,** using the Extract and Encrypt Master Key (XEM) command **116** described below (step **1704**). Referring also to FIG. 18, this command **116** encrypts the key part in question ("source key") under the transport key BTK in register **1614** and places the result in EBX register **1616,** where it is freely available to the requesting authority **104**; a hash pattern of the extracted key is also placed in BXHP register **1618.**
>
> Thereafter, the authority loads the key part that it has obtained in encrypted form into the appropriate master key register of the target module **102,** using the Load Key Part (LKP) command **116** described below (step **1706**). Referring also to FIG. 19, this command **116** decrypts the key part under the transport key BTK in the register **1614** of the target module **102** and places the result in the appropriate master key register of that module." Smith, col. 16, lines 10-35.

Thus, the basic transport key stored in the BTK register **1614** is merely a secret key which is used to encrypt part of a master key. Nowhere does Smith teach or fairly suggest that the BTK register **1614** is an input/output scrambling register which separately stores scrambling bits apart from a digital key with which the scrambling bits are previously intermixed. Indeed, the above-quoted text of Smith indicates that the BTK register **1614** is a dedicated register that only stores the basic transport key, and nothing else.

While Smith teaches performing encryption using the basic transport key, and also generating key hashes, nowhere does it teach or fairly suggest intermixing scrambling bits with a digital key to create digital key data, and then separately storing the scrambling bits in an input/output scrambling register for later use by a processing module to determine the digital key. As such, the selective combination of references proposed by the Examiner still fails to teach or fairly suggest all of the elements recited in the above-noted independent claims.

Accordingly, it is submitted that independent Claims 11, 17, 25, and 30 are patentable over the prior art. Their respective dependent claims, which recite yet further distinguishing features, are also patentable over the prior art and require no further discussion herein.

CONCLUSIONS

In view of the foregoing, it is submitted that all of the claims are patentable. Accordingly, a Notice of Allowance is respectfully requested in due course. Should any minor informalities need to be addressed, the Examiner is encouraged to contact the undersigned attorney at the telephone number listed below.

Respectfully submitted,

John F. Woodson

JOHN F. WOODSON, II
Reg. No. 45,236
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
Telephone: 407/841-2330
Fax: 407/841-2343
Attorney for Applicants